Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

The Information Commissioner's response to the Home Office consultation on the updated Surveillance Camera Code of Practice.

About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), among others.

The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

Introduction

As a statutory consultee, the Information Commissioner's Office (ICO) welcomes the opportunity to respond to the Home Office's public consultation on the updated Surveillance Camera Code of Practice. In this response, the Code of Practice issued under section 30 of the Protection of Freedoms Act 2012 (PoFA) will be referred to as 'the Code'.

The ICO recognises the significant benefits that surveillance systems can bring to people and businesses, from contributing to the security of the general public and property, to more focused contributions to assist the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This can also include the safeguarding against and the prevention of threats to public security. However, surveillance systems often capture high volumes of personal, sometimes sensitive data about individuals. These surveillance techniques can also play an influential role on how people may behave and move around freely in public spaces. Therefore, the public must have confidence that the use of surveillance systems is necessary and proportionate, and above all, lawful, fair, transparent and meets the other standards set out in data protection law.

General comments

It is important that the UK's updated data protection framework is referenced correctly within the Code. The EU GDPR is an EU Regulation and no longer applies to the UK. If an organisation operates inside the UK, they will need to comply with the Data Protection Act 2018 (DPA 2018). More specifically, the provisions of the EU GDPR have been incorporated directly into UK law and is now referenced as the UK GDPR. As a result, controllers in the UK will need to comply with both pieces of legislation and the ICO

recommends that any specific reference to GDPR within the Code should now read as UK GDPR.

In terms of accessibility, the ICO recommends that the Code seeks the most user friendly format. The overall structure of the Code may require improvements, and also practical examples throughout to assist the reader. The Code would also benefit from improved consistency of any language used relating to individuals' rights and disclosures, in keeping with that of data protection law.

The ICO welcomes that the Code requires any use of facial recognition or other biometric recognition systems to be clearly justified and proportionate. In keeping with the UK GDPR principle of lawful, fair and transparent processing, the Code would benefit from early expression and emphasis that any processing of personal data involving surveillance systems must indeed be 'lawful'. The Code may therefore require a definition of foreseeable lawful processing, and perhaps an additional technical definition of what live facial recognition is on page 5.

Where the Code (Principle 4) explores governance arrangements between jointly owned or jointly operated systems, the ICO recommends an emphasis on transparent responsibilities between joint controllers. This allows controllers to determine individual obligations, and would also assist individuals to efficiently exercise their rights and direct any correspondence to the appropriate controller. The Code may wish to reference ICO guidance on joint controllership[1] where relevant.

Under Principle 7 of the Code, the ICO recommends reference to the ICO's Data Sharing Code of Practice[2], especially where any disclosures may relate to onward sharing to law enforcement agencies or other authorised third parties. In addition, where the Code refers to considerations for disclosures under Principle 7, the ICO recommends that the Code emphasises that any considerations for disclosure should also be on a case by case basis, rather than being based solely on purpose.

Data protection by design / DPIAs

The ICO welcomes the detailed reference to Data Protection Impact Assessments (DPIAs) for any development or review of a surveillance system (Principle 2). Within this reference, it would be beneficial for the Code to provide additional weight to the legal requirement to perform a DPIA in most circumstances, and also refer to a risk based approach. For surveillance systems that process personal data in particular, controllers must perform a DPIA with balanced consideration for any type of processing that is likely to result in a high risk to individuals. To assess the level of risk, controllers should consider both the likelihood and the severity of any impact on individuals. The Code

[1] Controllers and processors | ICO
[2] Data sharing information hub | ICO

therefore may wish to link to specific ICO guidance pages in relation to DPIAs[3] and assessing risk.

Where the Code refers to consultation and engagement with the public and partners when assessing legitimate aims (Principle 3), the ICO suggests the outcomes of these consultations could also be recorded in a DPIA. This would be a useful addition to this particular point in the Code, in order to further encourage the completion of a comprehensive DPIA by controllers.

The framework for the use of live facial recognition (LFR)

The ICO notes that this is a small addition to the Code, despite the use of live facial recognition (LFR) technology in public spaces being a high profile method of processing the biometric data of large amounts of individuals. With reference to Principle 12 of the Code, the ICO recognises that the Court of Appeal judgment in the case of R (Bridges) v CC SWP suggests (at paragraph 118) that the Code could, in principle, i) "deal specifically with what the requirements are for inclusion on a police force's watchlist" and ii) "deal with what policies should contain in relation to the location of the deployment of AFR Locate". Based on the current draft of the Code, the section on the use of LFR appears light on detail and does not seem to follow these suggestions.

The ICO would be interested to learn more about whether the Home Office intends to include such content within any revisions of the Code or related products from the SCC, under the College of Policing's updated Authorised Professional Practice (APP) guidance, or elsewhere. Applying comprehensive updates to the Code directly, provides an opportunity for the suggestions within the judgment to be applied. Further, the ICO is interested to know if there will be a published roadmap to ensure that any other associated guidance products are signposted to users of LFR.

It is also important to note the Court's further requirement for there to be consistency between local policies (as suggested in paragraph 118 of the R (Bridges) v CC SWP judgement), and the ICO would appreciate further clarity surrounding the Home Office's intentions on that point in this Code.

Within Principle 12, the Code would also benefit from further detail in relation to the Public Sector Equality Duty. The Code's reference to 'potential adverse impact' and 'protected groups' is perhaps vague in relation to the Court's appetite for all police forces intending to use LFR "to satisfy themselves that everything reasonable which could be done had been done in order to make sure that the software used does not have a racial or gender bias (paragraph 201 of the Judgment)". The ICO would therefore welcome further detail, or examples, in the Code about how police forces could reduce any such adverse impacts on protected groups specifically in relation to racial or gender bias.

[3] Data protection impact assessments | ICO

Conclusion and future engagement

The ICO observes that the proposed updates to the new Surveillance Camera Code of Practice under the Protection of Freedoms Act 2012 (PoFA), particularly regarding the use of LFR, are not comprehensive. As mentioned earlier in this response, the ICO would welcome further clarity on whether any gaps in the Code are intentionally left for other products from the SCC, local police force policies, or national APP from the College of Policing. Again, a roadmap outlining different guidance products would be recommended and would assist users, especially in relation to LFR. Appropriate links or references to the Information Commissioner's formal Opinions[4] [5]on the use of LFR may also be a useful addition.

The ICO recommends a strengthened Code that recognises and anticipates potential future uses of surveillance systems, that could allow for the analysis of behaviour or profiling of individuals without any public debate. As the Code appears principle based, and neutral in terms of technologies, the ICO recommends that the Code should still attempt to identify any likely risks to the rights and freedoms of individuals in the future.

As always, we welcome the opportunity to further engage with the Home Office directly in the development of the Code where appropriate, or on any matters arising that may fall within the remit of the ICO.

Information Commissioner's Office

September 2021

[4] The use of live facial recognition technology by law enforcement in public places (ico.org.uk)
[5] Blog: Information Commissioner's Opinion addresses privacy concerns on the use of live facial recognition technology in public places | ICO